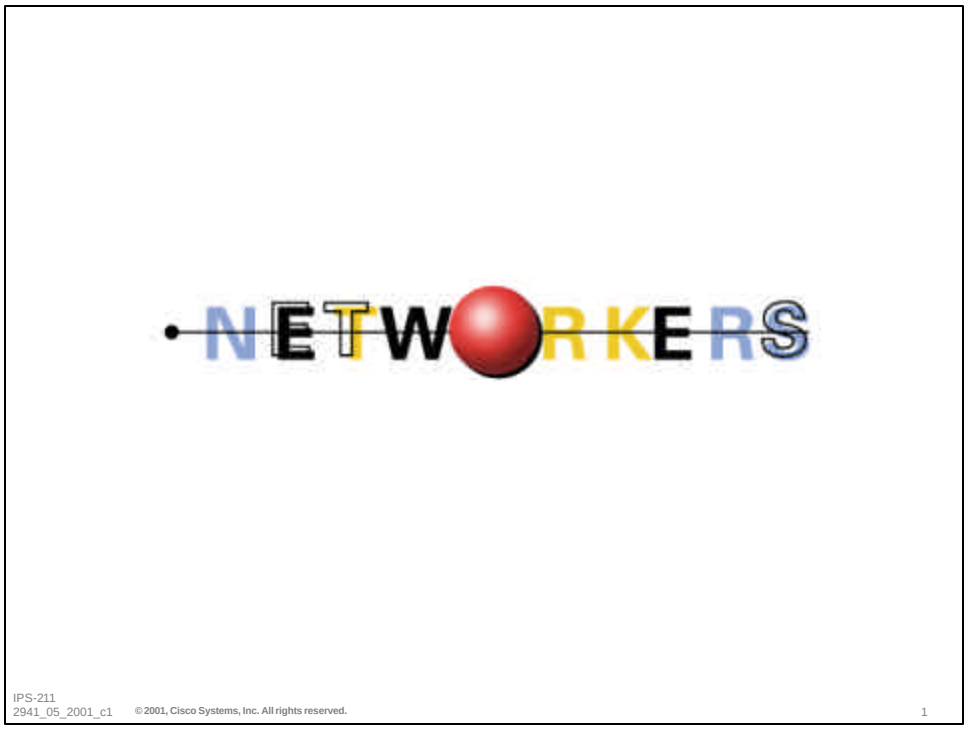
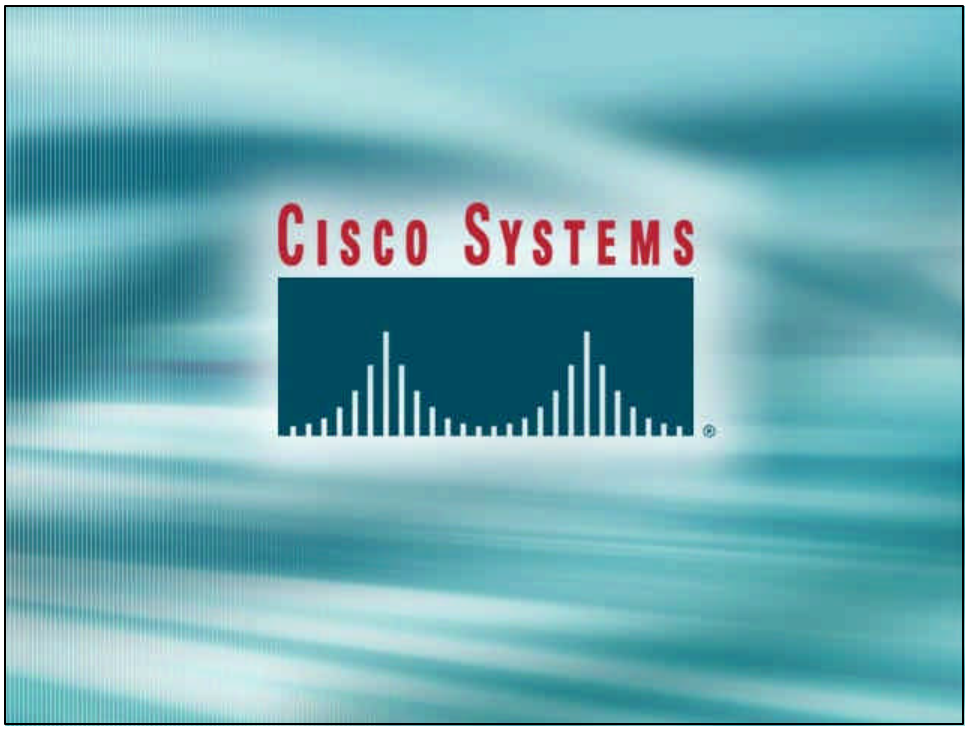




Cisco.com

Deploying Highly Resilient IP Networks

Session IPS-211

"The Janitor Pulled the Plug…"

Cisco.com

- Why was he allowed near equipment?
- Why was problem noticed only afterward?
- Why did it take 6 weeks to determine problem?
- Why wasn't there redundant power?
- Why wasn't there network redundancy?

What Is High Availability?

Cisco.com

When the Proportion of the Total Operating Time a Network Is Functional >= 99.999%

Availability	DPM	Downtime Per Year (24x7x365)		
99.000%	10K	3 Days	15 Hours	36 Minutes
99.500%	5K	1 Day	19 Hours	48 Minutes
99.900%	1000		8 Hours	46 Minutes
99.950%	500		4 Hours	23 Minutes
99.990%	100			53 Minutes
99.999%	10			5 Minutes
99.9999%	1			30 Seconds

Five 9's or More

How Do We Get There?

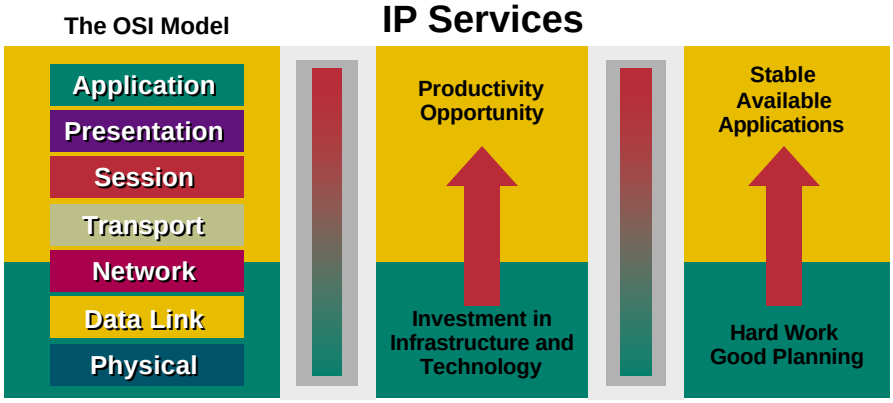
Cisco.com

"In the Internet era, reliability is becoming something you have to build, not something you buy. That's hard work, and it requires intelligence, skills and budget. Reliability is not part of the basic package."

Joel Snyder – Network World Test Alliance 1/ 10/00
"Reliability: Something you build, not buy"

Building Availability

Cisco.com



The Three-legged Stool

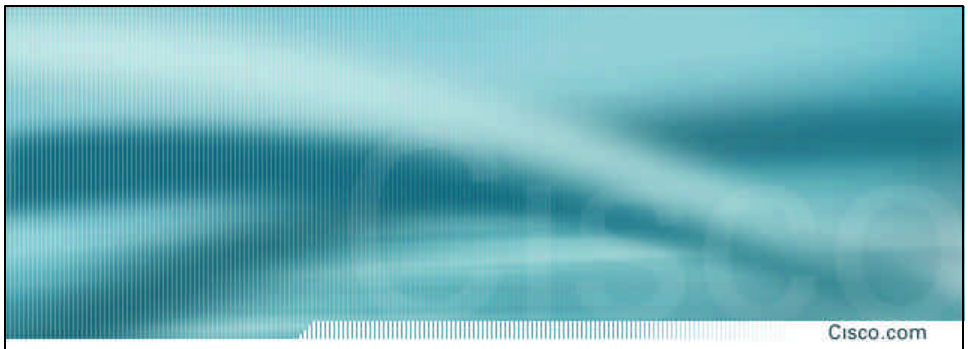
Cisco.com

- Designing the network with resiliency in mind
- Using technology to identify and eliminate single points of failure
- Having processes in place to reduce the risk of human error
- All of these elements are necessary, and all interact with each other


Design


Technology


Process



Design and Technology

The Basics: Platform and Environment

Cisco.com

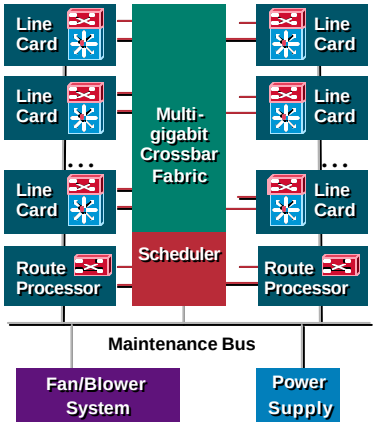
- Redundant power
- Redundant cooling
- 1:1 or N:1 card redundancy
- Redundant route processors
- Redundant switch fabric
- Environmental controls
- Power environment
- Cabling

Platform Redundancy: Cisco 12000 GSR

Technology

Cisco.com

- NEBS Level 3 compliant
- Automatic protection switching (APS)/Multiplex Section Protection (MSP)
- Hot swap capability
- Redundancy
  - Dual-route processors
  - Switch fabric redundancy
  - Redundant power supplies
  - Redundant cooling systems
  - Line card protection
- Maintenance bus

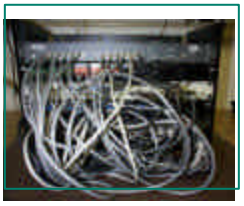


Effects of the Physical Plant

Design

Cisco.com

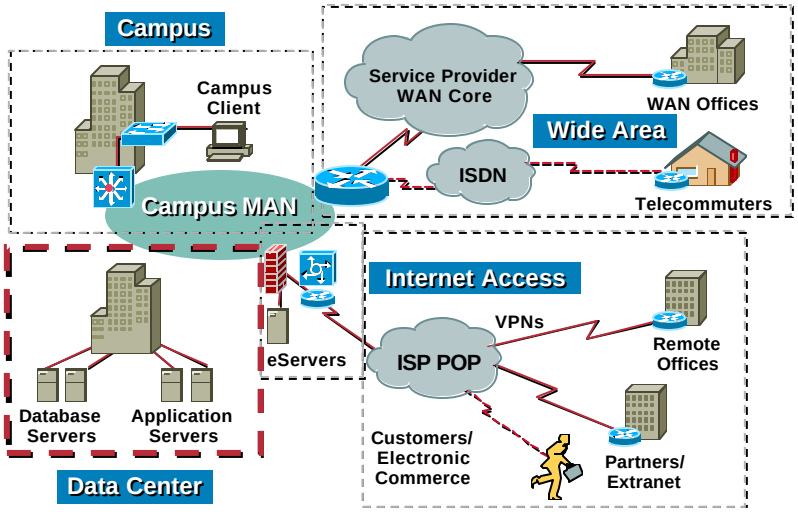
- MTBF
- Temperature/humidity /electronic noise
- Redundant power
- Color coding
- Device card/chassis access
- Cable labels
- Documentation
- Eliminate “The Janitor Effect”



Data Center Availability

Design

Cisco.com



IPS-211
2941_05_2001_c1

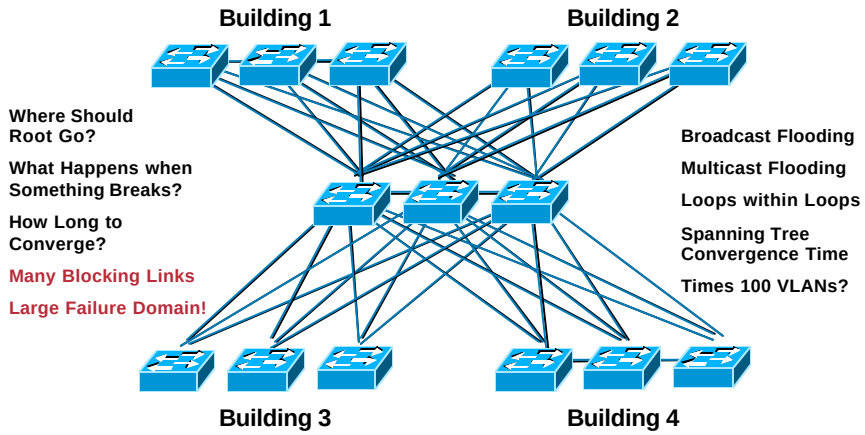
13

Backbone from Hell

Design

Cisco.com

Avoid Highly Meshed, Non-Deterministic Large Scale L2



Where Should Root Go?

What Happens when Something Breaks?

How Long to Converge?

Many Blocking Links

Large Failure Domain!

Broadcast Flooding

Multicast Flooding

Loops within Loops

Spanning Tree Convergence Time

Times 100 VLANs?

IPS-211
2941_05_2001_c1

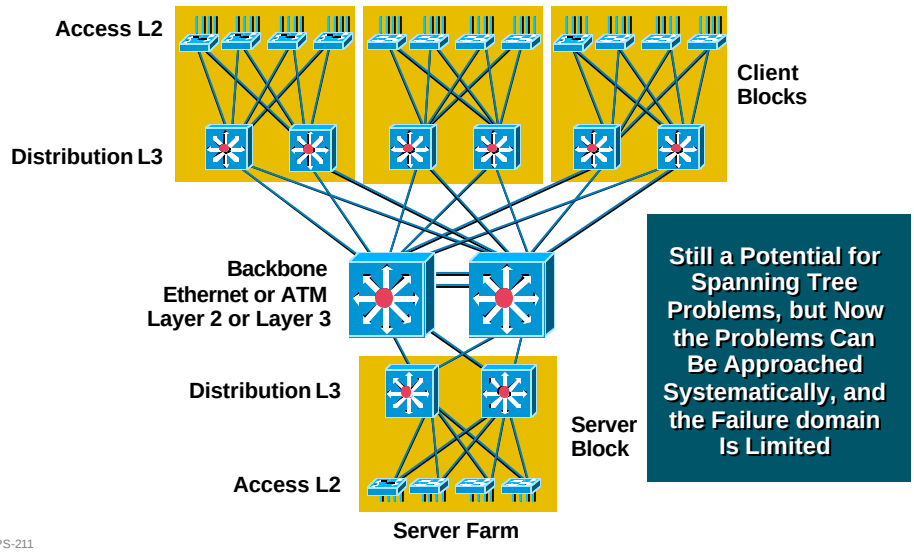
14

Presentation_ID.scr

Typical (Better) Backbone

Design

Cisco.com



Still a Potential for Spanning Tree Problems, but Now the Problems Can Be Approached Systematically, and the Failure domain Is Limited

Why Is Spanning Tree A Problem?

Design

Cisco.com

Spanning Tree State Machine

- **Blocking** — Time to Detect that Root Bridge Not Available: 20 secs
- **Listening** — Discarding Frames while Calculating New Root: 15 secs
- **Learning** — Discarding Frames while Learning Addresses: 15 secs
- **Forwarding** — Finally Forwarding Frames. To Reach this State: 50 secs

Accelerating STP Recovery

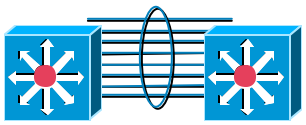
Cisco.com

- In a highly redundant L2 network, spanning tree recalculation can cause significant delays
- Two Cisco technologies can help alleviate this delay:
  - Ether Channel for fast or gigabit ethernet
  - Spanning tree optimizations: UplinkFast, PortFast and BackboneFast

EtherChannel®

Cisco.com

- Minimizes risk of link failure leading to spanning tree reconfiguration
- Increased availability
- Sub second recovery
- Single L2 STP link
- Single L3 subnet



Supported on the Catalyst Family as Well as Cisco IOS

Configuring EtherChannel

Cisco.com

On a Catalyst 6XXX:

```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 left admin_group 1.
Ports 2/2-8 joined admin_group 2.
Console> (enable)
```

On a Cisco 7500:

```
Router(config)# interface port-channel 1
Router(config)#  ip address 10.0.0.1 255.255.255.0
Router(config)#  ip route-cache distributed
Router(config)# interface fasteth 0/0
Router(config)#  no ip address
Router(config)#  channel-group 1
Router(config)# interface fasteth 0/1
Router(config)#  no ip address
Router(config)#  channel-group 1
FastEthernet 0/1 added as member-2 to fechannel1
```


Spanning Tree Optimizations

Cisco.com

PortFast: Allows a port on a switch to which an end station is attached to proceed directly to forwarding state

```
set spantree portfast 1/1 enable
set spantree portfast bpdu-guard enable
```

UplinkFast: Allows a wiring closet switch to transition a backup link directly into forwarding state

```
set spantree uplinkfast enable rate 40
```

BackboneFast: Allows a distribution or core switch to proactively seek out a new path to the STP root bridge

```
set spantree backbonefast enable
show spantree backbonefast
```

Reduce Unnecessary Peering

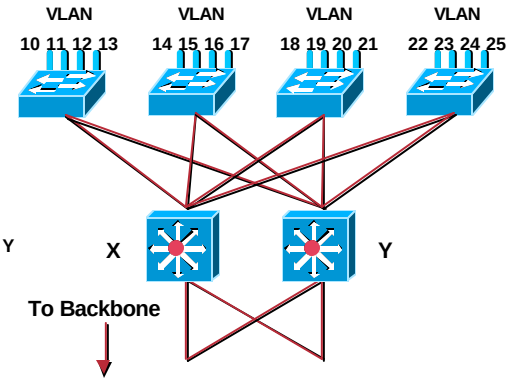
Design

Cisco.com

- Problem: Routers peer across each wiring closet VLAN
- Passive interfaces reduce peering overhead

4 VLANs per Wiring Closet
16 VLANs Total
16 Routed Paths between X and Y
Routing Overhead *16
Impacts Convergence Time

Solution: Make Wiring Closet VLAN Interfaces Passive on Routers X and Y



Using Passive Interfaces

Technology

Cisco.com

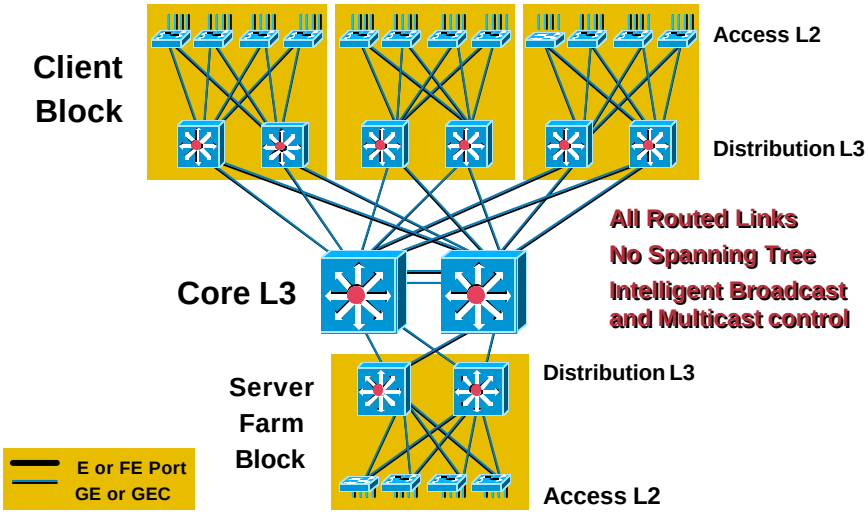
- Using passive interfaces at the distribution layer:
  - Reduces unnecessary peering
  - Speeds dykstra calculations
  - Speeds L3 convergence

```
interface Vlan31
 description Link to backbone
 ip address 10.31.0.81 255.255.0.0
 no ip directed-broadcast
 ip hello-interval eigrp 1 1
 ip hold-time eigrp 1 3
!
router eigrp 1
 passive-interface Vlan10
 passive-interface Vlan11
 passive-interface Vlan12
 passive-interface Vlan13
 passive-interface Vlan99
 network 10.0.0.0
```

Layer 3 Backbone

Design

Cisco.com



IPS-211
2941_05_2001_c1

23

Benefits of a L3 Backbone

Technology

Cisco.com

- Multicast PIM routing control
- Load balancing
- No blocked links
- Fast convergence EIGRP/OSPF
- Greater scalability overall
- Router peering reduced
- Cisco IOS features in the backbone

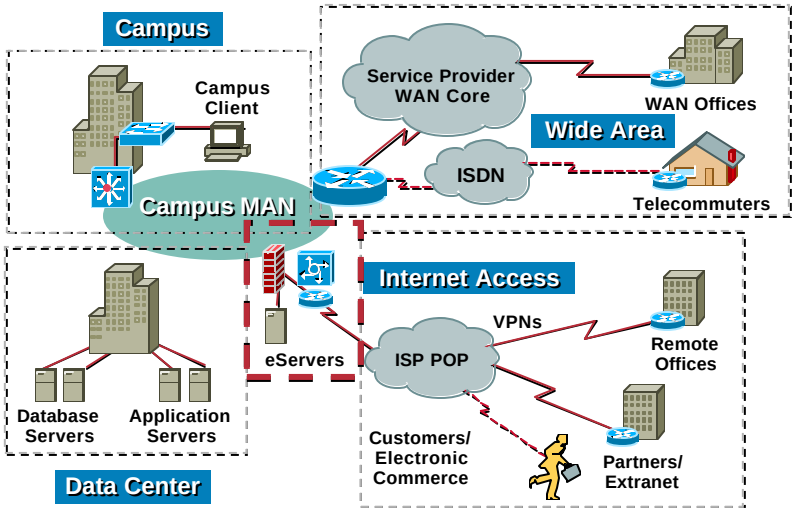
IPS-211
2941_05_2001_c1

24

Server Availability

Design

Cisco.com



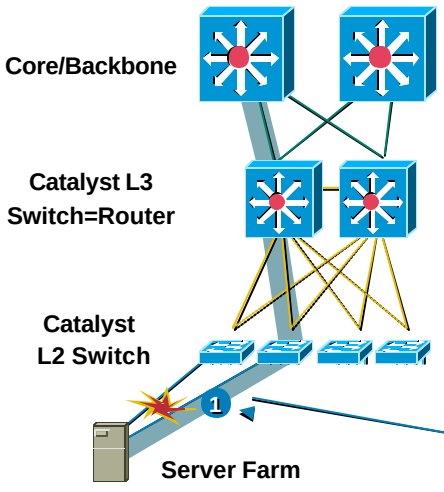
IPS-211
2941_05_2001_c1

25

Multi-homed Servers

Technology

Cisco.com



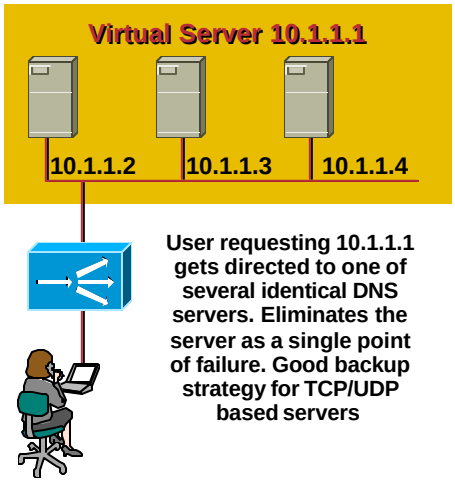
- Using Adaptive Fault Tolerant" Drivers and NICs
- NIC Has a Single IP/MAC Address (Active on one NIC at a Time)
- When Faulty Link Repaired, Does Not Fail Back to Avoid Flapping
- Fault-tolerant Drivers Available from Many Vendors: Intel, Compaq, HP, Sun
- Many Vendors also Have Drivers that also Support etherchannel

Dual-homed Server—Primary NIC Recovery (Time 1–2 Seconds)

IPS-211
2941_05_2001_c1

26

Redundant IP Servers Using Server Load Balancing



User requesting 10.1.1.1 gets directed to one of several identical DNS servers. Eliminates the server as a single point of failure. Good backup strategy for TCP/UDP based servers

```
ip slb serverfarm WEB-FARM
 real 10.1.1.2
 inservice
 real 10.1.1.3
 inservice
 real 10.1.1.4
 Inservice
!
ip slb vserver WEBSVR
virtual 10.1.1.1
serverfarm WEB-FARM
inservice
```

Requires either Cisco Local Director or an Cisco IOS SLB Image for the Cisco Catalyst 6XXX or the Cisco 7200

IPS-211
2941_05_2001_c1 27

SLB—Flexible Configurations

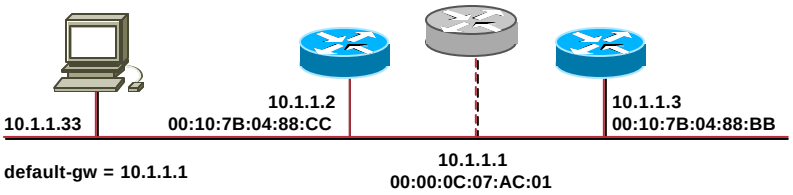
- Monitor the status of a server in a server farm and take it out of service
- Load-balancing between servers in a server farm
- Firewall load-balancing
- Redundant local directors
- Sticky connections
- Web Cache balancing
- WAP gateway balancing
- SYNGuard against DoS attacks
- Private and public servers
- NAT session redirection
- DNS, FTP, HTTP, HTTPS, IMAP, MATIP-A, NNTP, POP2/3, RealAudio/Video via HTTP, RADIUS, SMTP, Telnet, XOT

IPS-211
2941_05_2001_c1 28

HSRP—Hot Standby Router Protocol

Technology

Cisco.com



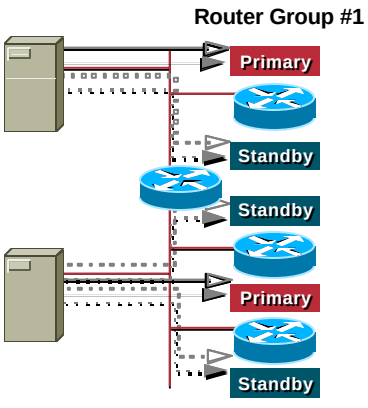
- Transparent failover of default router
- "Phantom" router created
- One router is active, responds to phantom L2 and L3 addresses
- Others monitor and take over phantom addresses

HSRP—RFC 2281

Technology

Cisco.com

- HSR multicasts hellos every 3 sec with a default priority of 100
- HSR will assume control if it has the highest priority and preempt configured after delay (default=0) seconds
- HSR will deduct 10 from its priority if the tracked interface goes down



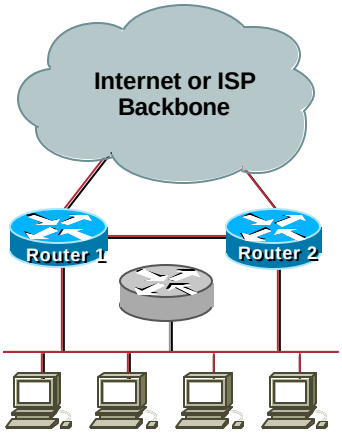
HSRP

Technology

Cisco.com

```
Router1:
interface ethernet 0/0
bandwidth 128
ip address 169.223.10.1 255.255.255.0
standby 10 ip 169.223.10.254

Router2:
interface ethernet 0/0
bandwidth 1500
ip address 169.223.10.2 255.255.255.0
standby 10 priority 150 pre-empt delay 10
standby 10 ip 169.223.10.254
standby 10 track serial 0 60
```

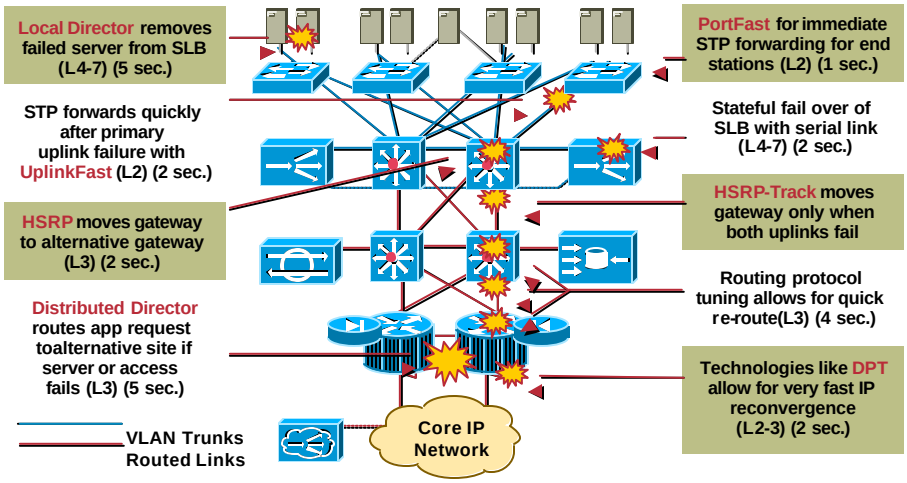


Putting All Of It Together

Design

Cisco.com

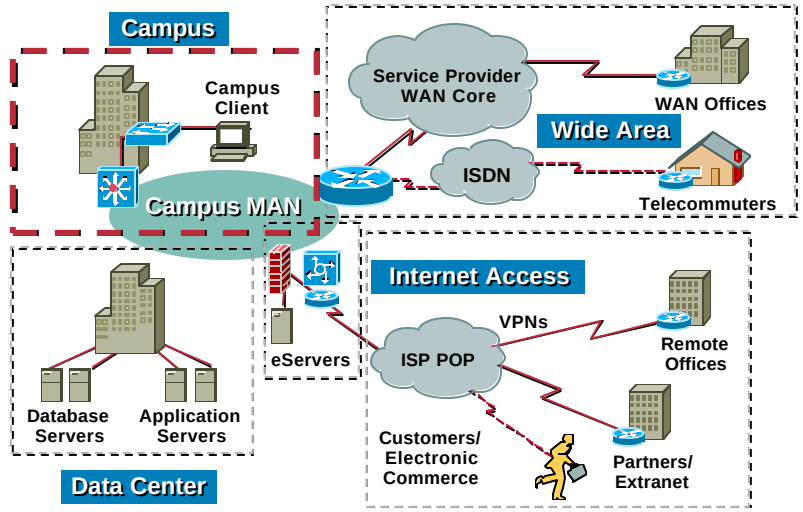
Resiliency Example



Campus Availability

Design

Cisco.com



Campus Backbone

Design

Cisco.com

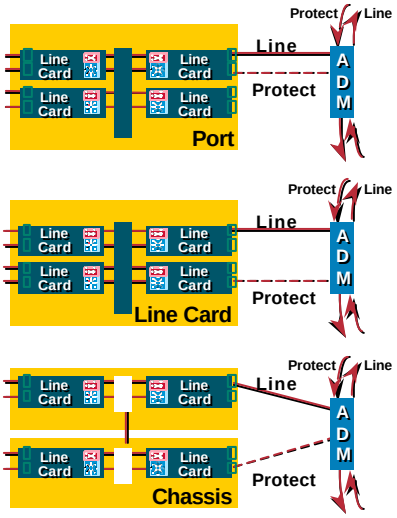
- Redundancy on the campus MAN varies depending on technology used
- Main choices are usually one of:
  - SONET/SDH
  - DPT/SRP
  - SRP or SONET/SDH over WDM
  - ATM
  - Gigabit Ethernet

SONET/SDH APS

Technology

Cisco.com

- Available on all SONET/SDH line cards
- Telcordia GR-253/ITU standards compliant
- K1/K2 link-layer control
- 3 levels of protection
  - Port failure
  - Line card failure
  - Router failure

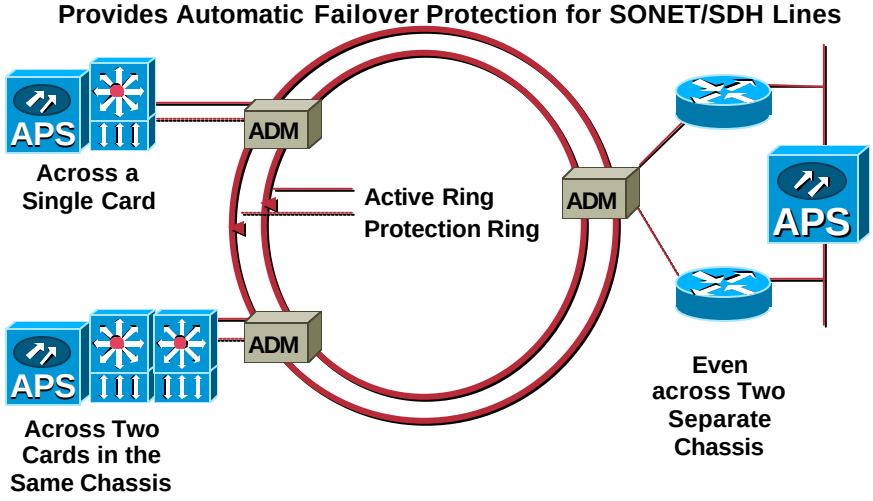


APS: Automatic Protection Switching

Technology

Cisco.com

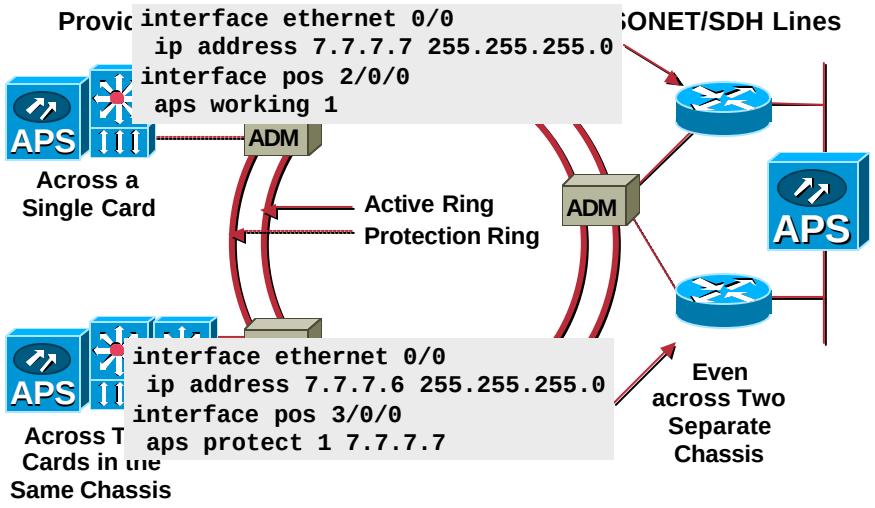
Provides Automatic Failover Protection for SONET/SDH Lines



APS: Automatic Protection Switching

Technology

Cisco.com

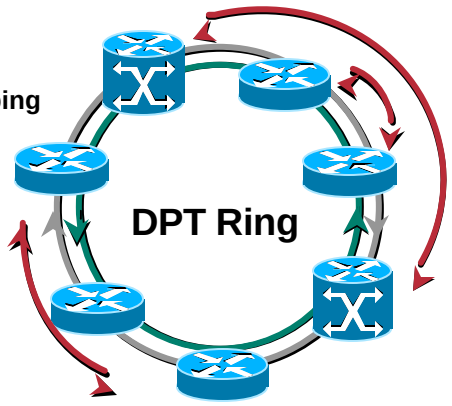


Dynamic Packet Transport

Design

Cisco.com

- No protection bandwidth as in SONET/SDH—uses ring wrap
- Bandwidth consumed only on traversed—destination stripping
- Multiple nodes transmit concurrently
- Fairness via SRP-fa
- Self-healing through IPS
- Multicast and prioritization support

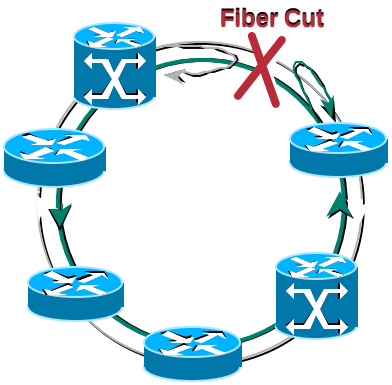


Intelligent Protection Switching

Technology

Cisco.com

- **Like SONET/SDH, DPT provides**
  - Proactive performance monitor and 50 ms self-healing via ring wrapping
- **Unlike SONET/SDH, DPT provides**
  - Signaling via explicit control messages
  - Multi-layer awareness and elastic cooperation
  - Differentiated handling by priority
  - Ring subnet, rather than point-to-point
  - Fast IP service restoration on large rings



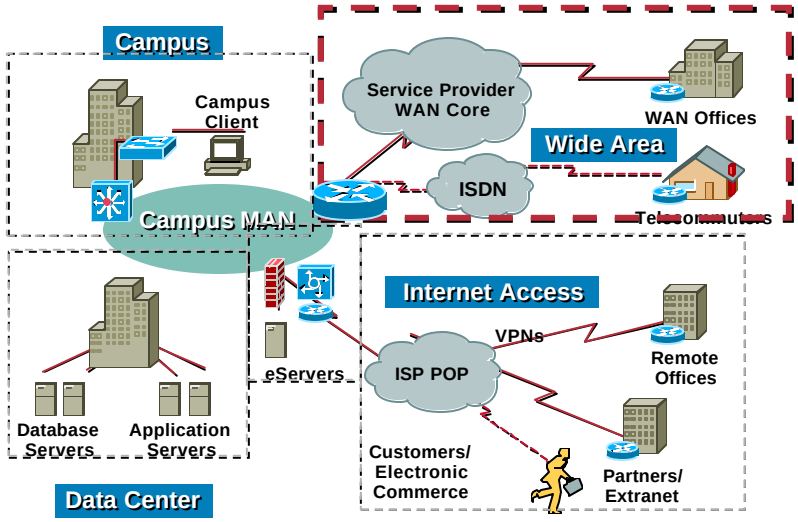
IPS-211
2941_05_2001_c1

39

WAN Availability

Design

Cisco.com



IPS-211
2941_05_2001_c1

40

Presentation_ID.scr

Circuit Diversity

Design

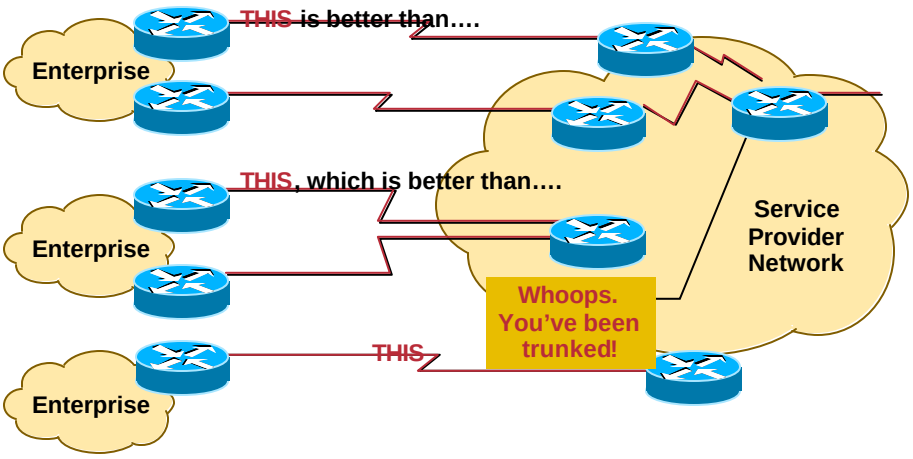
Cisco.com

- Having backup PVCs through the same physical port accomplishes little or nothing
- Port is more likely to fail than any individual PVC
- Use separate ports, preferably on separate routers
- Try to have it written into your SLA that your backup path terminates into separate equipment at the service provider, and that your lines are not trunked into the same paths as they traverse the network

Circuit Diversity

Technology

Cisco.com



Using MLPPP

Cisco.com

```
interface Multilink1
 ip address 172.16.11.1 255.255.255.0
 ppp multilink
 multilink-group 1
!
interface Serial1/0
 no ip address
 encapsulation ppp
 ppp multilink
 multilink-group 1
!
interface Serial1/1
 no ip address
 encapsulation ppp
  ppp multilink
 multilink-group 1
```

Multi-link PPP, if employed with proper circuit diversity, can provide redundancy to TDM lines.
Has the value-added effect of increasing your bandwidth

MLPPP Bundle

Load Sharing

Cisco.com

- Load sharing occurs when a router has two (or more) equal cost paths to the same destination
- EIGRP also allows unequal-cost load sharing
- Load sharing can be on a per-packet or per-destination basis (default: per-destination)
- Load sharing can be a powerful redundancy technique, since it provides an alternate path should a router fail

Load Sharing

Cisco.com

- OSPF will load share on equal-cost paths by default
- EIGRP will load share on equal-cost paths by default, and can be configured to load share on unequal-cost paths:

```
router eigrp 111
 network 10.1.1.0
 variance 2
```

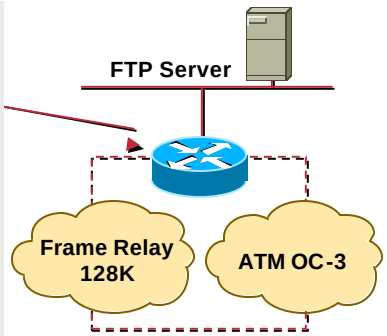
- Unequal-cost load-sharing is discouraged; Can create too many obscure timing problems and retransmissions

Policy-based Routing

Cisco.com

- If you have unequal cost paths, and you don't want to use unequal-cost load sharing (you don't!), you can use PBR to send lower priority traffic down the slower path

```
! Policy map that directs FTP-Data
! out the Frame Relay port. Could
! use set ip next-hop instead
route-map FTP_POLICY permit 10
   match ip address 6
   set interface Serial1.1
!
! Identify FTP-Data traffic
access-list 6 permit tcp any eq 20 any
!
! Policy maps are applied against
! inbound interfaces
interface ethernet 0
   ip policy route-map FTP_POLICY
```



BGP Multi-path Load Sharing

Technology

Cisco.com

- If two identical eBGP paths are learned from the same neighboring AS, and maximum-paths is greater than 1, install up to maximum-paths into the routing table
- Otherwise, use the lowest router-id to break the tie, and install just a single route
- Up to 6 maximum-paths routes are permitted

```
router bgp 109
  network 131.108.0.0
  network 192.31.7.0
  neighbor 131.108.200.1 remote-as 167
  maximum-paths 3
```


Convergence

Design

Cisco.com

- The convergence time of the routing protocol chosen will affect overall availability of your WAN
- Main area to examine is L2 design impact on L3 efficiency
- For detailed comparisons of OSPF, EIGRP:

  RST-207 deploying OSPF

  RST-209 deploying EIGRP

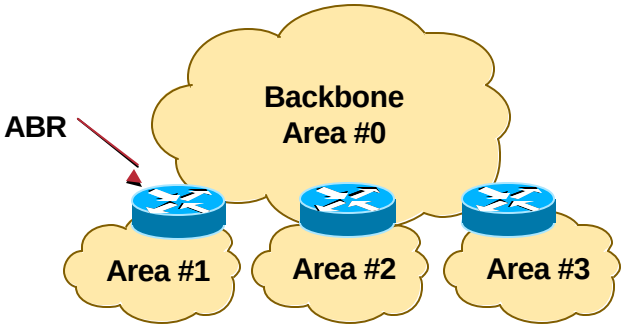
Factors Determining Protocol Convergence

Cisco.com

- Network size
- Hop count limitations
- Peering arrangements (edge, core)
- Speed of change detection
- Propagation of change information
- Network design: hierarchy, summarization, redundancy

OSPF—Hierarchical Structure

Cisco.com



- Topology of an area is invisible from outside of the area
  - LSA flooding is bounded by area
  - SPF calculation is performed separately for each area

Methods to Improve OSPF Scaling

Technology

Cisco.com

- **Route summarization**

On ABR:

```
router ospf 100
area 1 range 128.213.64.0 255.255.224.0
```

On ASBR:

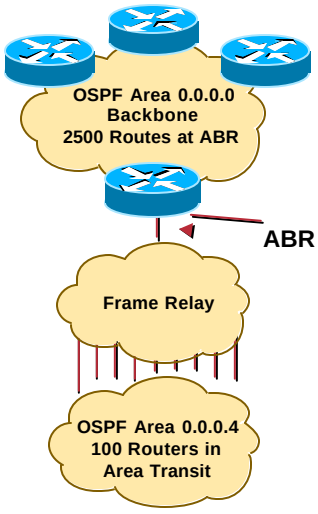
```
router ospf 100
summary-address 128.213.96.0 255.255.224.0
```

- **Stub or not so stubby areas (NSSA)**

OSPF Scaling

Design

Cisco.com



2500 Routes/
~46 Routes per Summary LSA

~54 1500-Byte Packets Required*
100 Routers

5400 Packets*
1500 Bytes

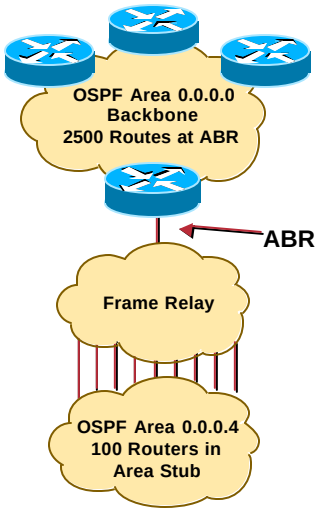
8100000 Bytes*
8 Bits =

~64.8 Mbps Bandwidth Requirement

OSPF Scaling—Stub Areas

Technology

Cisco.com



52 Bytes Per Default-Route Packet*
100 Routers

5200 Bytes*
8 Bits =

~41.6 Kbps Bandwidth Requirement

```
router ospf 1
network 10.3.1.0 area 0
network 10.3.2.0 area 4
area 4 stub no-summary
```

IPS-211
2941_05_2001_c1 53

EIGRP—Convergence

Design

Cisco.com

- EIGRP will track successor routes (alternate routes to be used in case of failure)
- If a successor route is found, switchover occurs with no interaction with other routers; immediate convergence
- If no feasible successor routes exist, router sends a query to neighbors to find a route
- Because queries can stretch to the very edge of the network, makes sense to limit their scope

IPS-211
2941_05_2001_c1 54

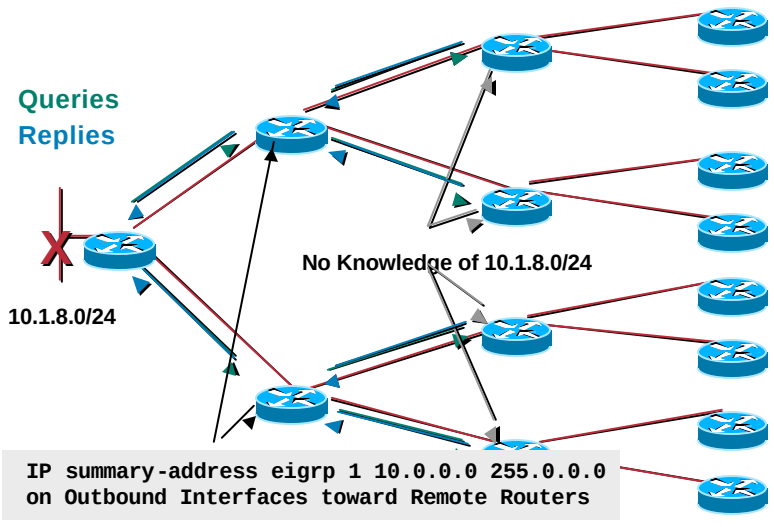
Decreasing Query Scope

Technology
Cisco.com

- **Summarization (manual or auto)**
- **Distribute-lists**
  - **Particularly on dual-homed remotes**
- **Stub routers (release 12.0S)**
  - **Signals HUB router not to send queries**

Decreasing Query Scope with Summarization

Technology
Cisco.com

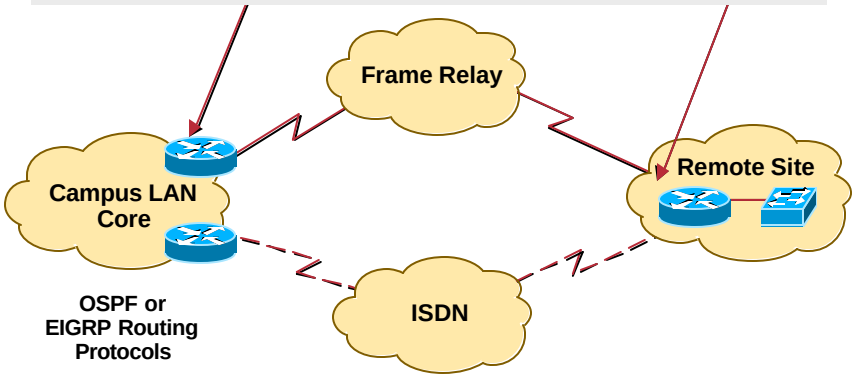



```
IP summary-address eigrp 1 10.0.0.0 255.0.0.0
on Outbound Interfaces toward Remote Routers
```

Dial Backup

Technology
Cisco.com

```
map-class frame-relay vcgrp router1
 frame-relay end-to-end keepalive mode bidirectional
```



Dial Backup

Technology
Cisco.com

```
!--- password for other router defined
username ROUTER2 password 0 letmein
!
interface Serial0.1
 ip address 172.16.2.1 255.255.255.128
 frame-relay interface-dlci 102
!
interface BRI0
 description ISDN for frame relay
 ip address 172.16.3.1 255.255.255.0
 encapsulation ppp
 dialer map ip 172.16.3.2 name ROUTER2 broadcast 6234020
 dialer-group 1
!--- Floating static route defined below
ip route 172.16.4.0 255.255.255.0 172.16.3.2 200
!
!--- Dialer list defines interesting traffic
dialer-list 1 protocol ip list 101
!
```

VPN Backups

Design

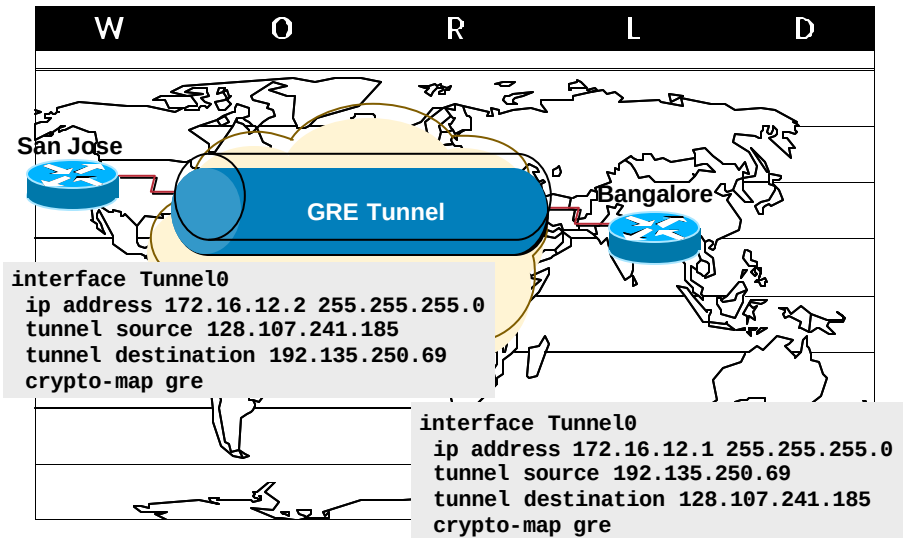
Cisco.com

- If WAN and internet access are separate, the internet can be leveraged as a backup path
- Since a tunnel will traverse the internet, some level of encryption is needed
- Many variations: L2TP, GRE, IPSec
- If you want to encrypt (you do…), need encryption—enabled version of IOS

Site-to-Site VPN Example

Technology

Cisco.com




```
interface Tunnel0
 ip address 172.16.12.2 255.255.255.0
 tunnel source 128.107.241.185
 tunnel destination 192.135.250.69
 crypto-map gre
```

```
interface Tunnel0
 ip address 172.16.12.1 255.255.255.0
 tunnel source 192.135.250.69
 tunnel destination 128.107.241.185
 crypto-map gre
```

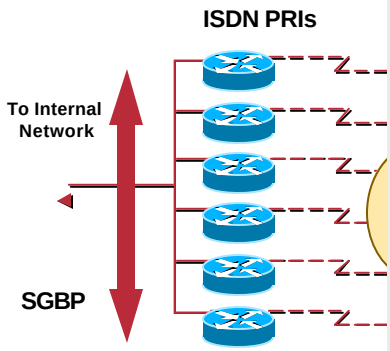
Adding Encryption

Cisco.com

```
crypto isakmp policy 10
authentication pre-share
!
crypto isakmp key cisco123 address 192.135.250.69
!
crypto ipsec transform-set one esp-des esp-md5-hmac
mode transport
!
crypto map gre 10 ipsec-isakmp
set peer 192.135.250.69
set transform-set one
match address gre1
!
ip access-list extended gre1
permit gre host 192.135.250.69 host 128.107.241.185
```


Multi-chassis MLPPP

Cisco.com

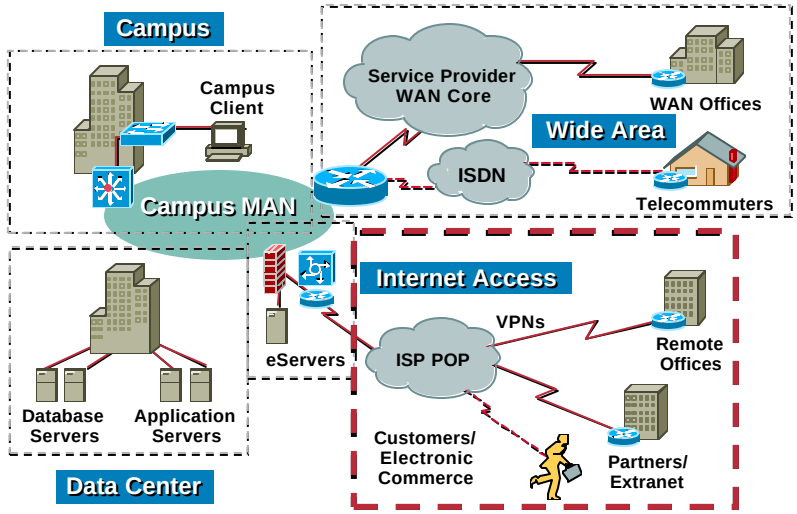



```
sgbp group stackq
sgbp member systemb 1.1.1.2
sgbp member systemc 1.1.1.3
!
username stackgroup password cisco
!
isdn switch-type primary-4ess
controller t1 0
 framing esf
 linecode b8zs
 pri-group timeslots 1-23
!
interface Serial0:23
ip unnumbered e0
 dialer map .....
 encapsulation ppp
 ppp authentication chap
 dialer-group 1
 dialer rot 1
!
ppp multilink
```

Internet Availability

Design

Cisco.com



Many of the Same Rules Apply

Design

Cisco.com

- Routing to the internet is not significantly different than routing to any other WAN site
- Ensure proper circuit diversity
- Protect dual paths with HSRP and track interface
- Optimize routing via load-sharing and fast convergence

Do I Need BGP?

Cisco.com

Questions to Ask:

Do I have more than one co-located paths to the Internet

And

Do I, for cost, security or other administrative reasons, need to selectively route (or have traffic routed to me) over one path rather than the other?

When Not to Use BGP

When you have a single path to the Internet. Use a static default route instead

When you have two paths to the internet but you don't care which way your traffic goes. Use two default routes (and possibly load-balance)

"My ISP says I need to use BGP so he can get the routes from my AS"

Run BGP, send your routes, but request that the ISP send you no routes. Use a default route

BGP Route Refresh Capability RFC2918

Cisco.com

- Facilitates non-disruptive policy changes—i.e. don't have to clear bgp session
- No configuration is needed
- No additional memory is used
- Clear ip bgp x.x.x.x in | out
- "in" => send route-refresh (new BGP message—type 5) request to neighbor
- "out" => withdraw and resend all routes to peer, via new policy

Cisco.com

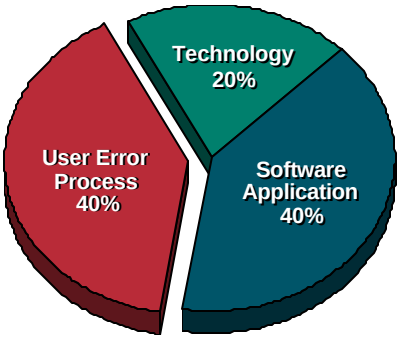
Operational Excellence

User Error/Process

Process

Cisco.com

- Change management
- Process consistency
- Capacity management
- Configuration management
- Network security
- Change management



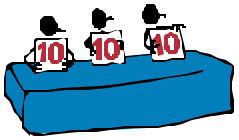
Source: Gartner Group

Process Goals

Process

Cisco.com

- Consistent speedy repair times
  - Configuration management
  - Fault management
  - Performance management
- Quality improvement
  - Availability metrics
  - Fault management metrics
  - Root-cause analysis
  - Performance indicators



Process Goals

Process

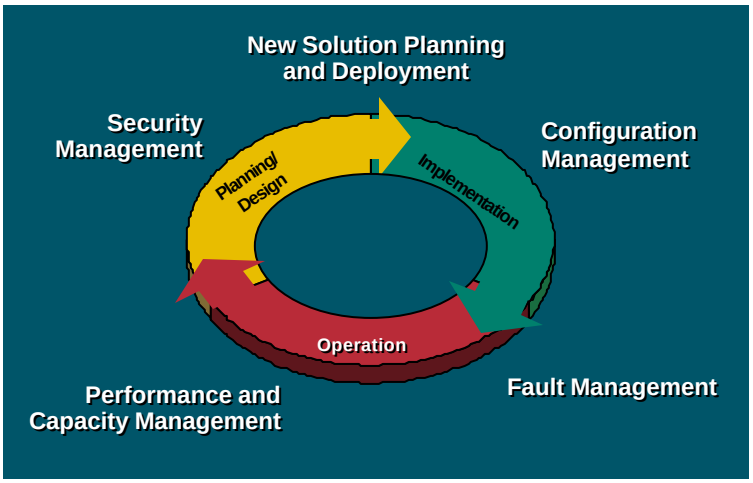
Cisco.com

- Problem avoidance
  - Network design and resiliency
  - Security
  - Proactive fault management
  - Capacity and performance management
- Successful network evolution
  - Change planning management
  - Testing and validation

Network Life-Cycle Management

Process

Cisco.com



New Solution Deployment

Process

Cisco.com

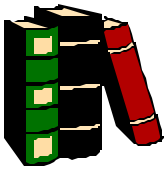
- Design review with vendor
- Test plan (to reflect your app/network scenarios)
- Lab validation
- Solution pilot
- Solution templates
- Staffing
- Training
- Operational support handoff

Configuration Management

Process

Cisco.com

- Maintaining configuration consistency
- Inventory management
- IP address management
- Software version control
- Password management
- Wiring and naming conventions
- Documentation

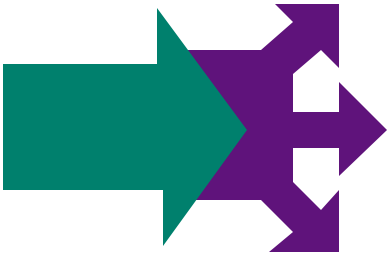


Configuration Management

Process

Cisco.com

- Change Management
  - Change management procedures
  - Risk analysis
  - Testing/validation for high risk change
  - Backout plan
  - Network management and documentation update
  - Change management metrics



Performance and Capacity Management

Cisco.com

- Base-lining
- What-if analysis (network and application)
- QoS management
- Periodic review plan and upgrade criteria
- Exception management

Fault Management

Cisco.com

- Fault management

  24 x 7 detection, notification, escalation, resolution for link/hardware/network failures

  Proactive fault analysis plan (MIB variables, threshold violations, syslog events, review plan)

  Infrastructure (TFTP, syslog, NTP, time-stamps, out-of-band management, vendor access)

  Help desk systems (metrics, accountability)

Security Management

Cisco.com

- Internet access
- Dial-in access
- Partner access
- Security operations
- Internet/partner monitoring
- CERT/vendor advisory review
- Security configuration practices
- Termination practices

Process Tools

Cisco.com

CiscoWorks Resource Manager Essentials
Configuration/Change/Inventory Management

CiscoWorks Device Fault Manager
Fault Mgmt

CiscoWorks Secure Policy Manager
Security Mgmt

Cisco NetFlow Accounting
Accounting and Capacity Mgmt

Interfaces to Oracle/Remedy
Problem Mgmt

CiscoWorks Internetwork Performance Monitor
Performance Mgmt

Cisco Management Connection

Cisco.com

http://wwwin.cisco.com/cmc/cc/pd/wr2k/ent/

In Summary

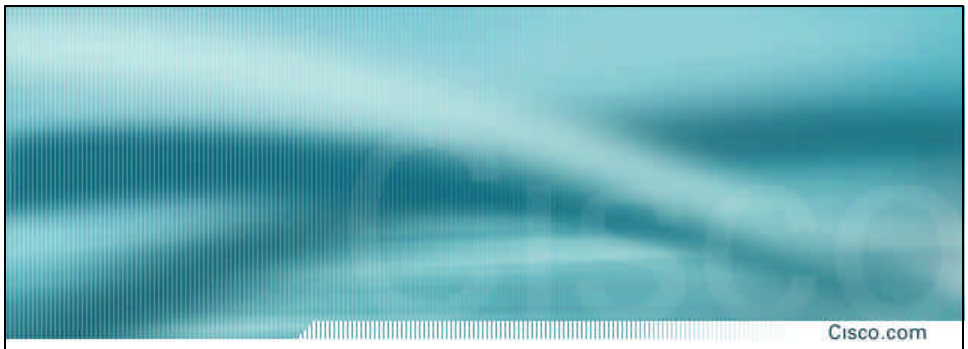
Cisco.com

- Implementing a highly resilient IP network requires a combination of the proper process, design and technology
- "and now abideth design, technology and process, these three; but the greatest of these is process"


Design

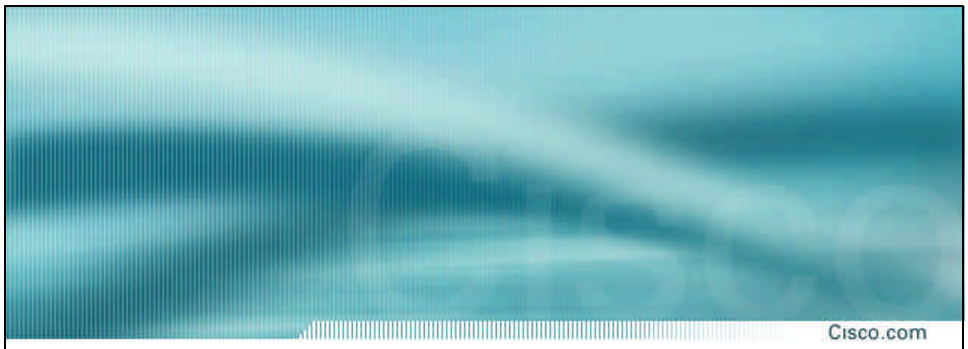

Technology


Process



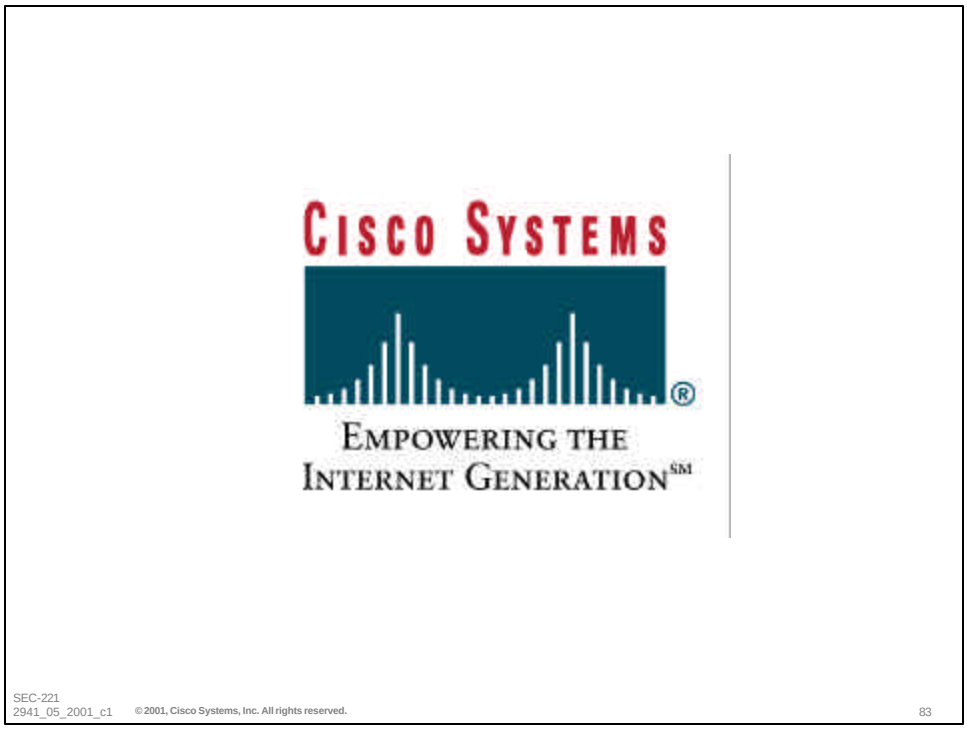
Deploying Highly Resilient IP Networks

Session IPS-211



Please Complete Your Evaluation Form

Session IPS-211



SEC-221
2941_05_2001_c1 83